Содержание:

ВВЕДЕНИЕ

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации.

Новые информационные технологии бурными темпами внедряются во все сферы деятельности жизни людей. Появление локальных и глобальных сетей передачи данных предоставило пользователям компьютеров новые возможности оперативного обмена информацией. Если до недавнего времени подобные сети создавались только в специфических и узконаправленных целях (университетские сети, сети военных ведомств, спецслужб и так далее), то развитие Интернета и аналогичных систем привело к использованию глобальных сетей передачи данных в повседневной жизни практически каждого человека. Информация, как ресурс, несет в себе значительную ценность, поэтому при нынешней информатизации общества очень важно сохранить целостность и неприкосновенность передаваемой информации.

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Начало формы

Конец формы

Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на три основных типа:

— перехват информации — целостность информации сохраняется, но её конфиденциальность нарушена;

— модификация информации — исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату;

— подмена авторства информации. Данная проблема может иметь серьёзные последствия. Например, кто-то может послать письмо от вашего имени (этот вид обмана принято называть спуфингом) или Web — сервер может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не высылать никаких товаров.

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Угрозы информационной безопасности — это оборотная сторона использования информационных технологий.

Выборочная и бессистемная реализация мероприятий, направленных на повышение уровня IT-безопасности, не сможет обеспечить необходимого уровня защиты. Чтобы сформировать понимание приоритетности мероприятий по повышению уровня безопасности, необходимо разработать механизм управления рисками IT-безопасности, что позволит направить все усилия на защиту от наиболее опасных угроз и минимизацию затрат.

Актуальность и важность проблемы обеспечения информационной безопасности обусловлена следующими факторами:

− увеличение рисков информационной безопасности в связи с появлением новых и изощренных угроз для информационной безопасности;

− современные темпы и уровни развития средств информационной безопасности значительно отстают от темпов и уровней развития информационных технологий;

− быстрые темпы роста парка персональных компьютеров, применяемых в разнообразных сферах человеческой деятельности из-за увеличения

обрабатываемой информации;

− резкое расширение сферы пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;

− доступность корпоративной информации через мобильные устройства (ноутбук, КПК, смартфон).

− доступность средств персональных ЭВМ, привела к распространению компьютерной грамотности в широких слоях населения.

− значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации.

− стремительное развитие информационных технологий, открыло новые возможности эффективной работы предприятия, однако привело и к появлению новых угроз.

Анализа угроз информационной безопасности позволяет определить, какие мероприятия эффективны для их минимизации и предотвращения, а какие нет.

Цель данной работы состоит в определении видов угроз информационной безопасности и их состава.

Структура курсовой работы. Курсовая работа состоит из введения двух глав, заключение и списка использованных источников.

ГЛАВА 1. КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Основные понятия теории информационной безопасности

Информация—это сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством для нужд человека. Информация необходима каждому как условие и как средство существования человека в обществе. И поэтому так же нуждается в защите, как среда обитания,

пища и все остальные элементы жизнедеятельности.

Стремительное нарастание возможностей оперативного обмена экономической, научно-технической, культурной, политической, военной и другой информацией является несомненным благом, великим достижением цивилизации.

В третьем тысячелетии, на фоне перехода человечества от индустриальной цивилизации к цивилизации информационной, информация стала одним из главных факторов исторического прогресса. Она имеет ключевое значение для успешного функционирования всех общественных и государственных институтов, адекватного поведения каждого отдельного человека. Без интенсивного обмена информацией, постоянной информационной связи с окружающим миром в принципе невозможна нормальная жизнедеятельность людей.

Однако, как известно, любое благо в определенных условиях или при неправильном использовании может перерасти в беду.

Например, прекращение информационных контактов с социальной средой, как правило, ведет к личностной деградации человека, становится источником различных отклонений – вплоть до психических расстройств.

Прогресс в любой сфере является позитивным и полезным до определенного предела, за которым его результаты могут оказаться вредными. Так, развитие информационных технологий вызвало одновременно расширение возможностей массовой дезинформации – введения в заблуждение огромных масс людей путем сообщения неверных сведений, подтасовки фактов, подделки доказательств.

В итоге современное общество образуют не только информированные, то есть хорошо осведомленные о чем-либо, люди, но и дезинформированные – введенные в заблуждение ложной информацией. Каких из них больше – неизвестно. Наряду с информированием людей постоянная дезинформация (а проще – обман, ложь) также стала нормой жизни во многих сообществах и странах. Она широко используется как информационное и психологическое оружие в международной политике, в идеологической обработке людей, в интересах экономической экспансии, для ослабления национально-государственного самосознания граждан, разрушения семей, корпораций и государств.

О роли влияния информационных факторов на жизнедеятельность современного общества говорит тот факт, что созданный человечеством в природной среде «искусственный мир» образует уже не только техносфера (мир техники,

технологий, сооружений и т. п.), но и информационная сфера, значимость которой для жизни каждого из нас непрерывно возрастает.

Доктрина информационной безопасности РФ определяет информационную сферу как совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

В наиболее общем виде информационную сферу (или информационную среду) образуют:

- субъекты информационного взаимодействия или воздействия (люди, организации, системы);
- собственно, информация, предназначенная для использования субъектами информационной сферы;
- информационные технологии и технические средства;
- информационная инфраструктура, обеспечивающая возможность осуществления обмена информацией между субъектами;
- общественные отношения, складывающиеся в связи с формированием, передачей, распространением и хранением информации, и система их регулирования.

Согласно Доктрине информационной безопасности РФ, под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В специальной литературе используется более широкое определение: информационная безопасность – это такое состояние социума, при котором обеспечена надежная и всесторонняя защита личности, общества и государства от воздействия на них особого вида угроз, выступающих в форме организованных информационных потоков и направленных на деформацию общественного и индивидуального сознания.

Понятие «информационная безопасность» сегодня трактуется как в широком, так и в узком смысле. В широком смысле – это информационная безопасность человека, общества и государства. В узком смысле – это безопасность самой информации и каналов ее приема (передачи), а также организация защиты от применения противником информационного оружия в ходе боевых действий.

Понимание безопасности в контексте соотношения интересов личности, общества и государства предполагает рассмотрение информационно-психологической безопасности как аспекта общей проблемы.

Информационно-психологическую безопасность в общем виде можно определить, как состояние защищенности индивидуальной, групповой и общественной психологии социальных субъектов различных уровней общности от разрушительного воздействия на сознание негативных информационных факторов.

Применительно к конкретному человеку информационно-психологическая безопасность – это состояние защищенности сознания и психического здоровья человека, обеспечивающее его целостность как социального субъекта, возможность адекватного поведения и личностного развития в условиях неблагоприятных информационных воздействий.

Информационное противоборство—это комплексное взаимное информационное воздействие сторон друг на друга, которое способно привести к принятию благоприятных для инициатора воздействия решений либо парализовать информационную инфраструктуру противника. Методы воздействия: радиоэлектронная борьба, компьютерные конфликты, действия на психологическом и мировоззренческом уровнях, вброс ложной или компрометирующей информации, внушение, навязывание и т. п.

Более острая стадия противоборства – информационная война – согласованная деятельность по использованию информации как оружия для разрушающего воздействия на противника в различных сферах: экономической, политической, социальной и на поле боя. Информационная война – война нового типа, ее основным объектом являются не только информационные системы, но, прежде всего, сознание людей, их поведение и здоровье.

В информационной войне для разрешения межгосударственных противоречий и конфликтов используются методы и средства силового воздействия на сознание общества и информационную сферу государств. Информационные войны могут происходить и внутри страны, например, при столкновении политических и экономических противников, в ситуациях обострения борьбы за власть, при проведении избирательных кампаний, судебных процессов и т. п.

Термин «информационная война» известен давно, но стал широко употребляться американскими специалистами после завершения войны с Ираком (1991–1992 гг.), где информационное оружие показало свою высокую эффективность. В 1992 г.

Пентагон уже издал директиву «Информационная война» (TS 3600.1), в которой намечались основные задачи по подготовке к такого рода войнам, их методы и средства.

Основные цели и задачи информационной войны:

- подавление и уничтожение систем управления противоборствующей стороны;
- информационное обеспечение боевых действий, политики, экономики;
- подавление электронных систем противника;
- психологическое воздействие на личный состав и население;
- хакерское проникновение в информационные системы противника.

Информационная угроза—опасность, содержание которой составляют различная информация или ее комбинации, которые могут быть использованы против социального или социально-технического объекта (системы) с целью изменения его интересов, потребностей, ориентаций в соответствии с целями субъекта информации.

Информационный риск – вероятность информационной угрозы и реальных действий противника, мера измерения успешности или опасности возможных воздействий. Риск зависит от характера воздействий и объекта воздействий, от условий их осуществления, а также от возможностей защиты.

Составным элементом информационных войн является информационная операция. В зависимости от характера объектов и средств воздействия информационные операции подразделяются на информационно-технические и информационно-психологические.

Наступательную информационную операцию, осуществляемую вероломно и преследующую корыстные и даже преступные цели в отношении человека или общества можно определить как информационную агрессию.

Оборонительная информационная операция включает мероприятия по обеспечению безопасности собственных информационных ресурсов:

- оперативную и стратегическую маскировку;
- сохранение секретов;
- контрразведку;
- физическую защиту объектов информационной инфраструктуры;
- глушение, блокирование СМИ противника;

- контрпропаганду;
- психотерапию;
- контрдезинформацию;
- радиоэлектронную борьбу.

Ведение информационных войн предполагает наличие и использование определенных средств борьбы, то есть оружия.

Под информационным оружием понимается совокупность специально организованной информации, а также информационных технологий, применяемая для деструктивных воздействий на поведение и сознание населения, персонал эргасистем, военнослужащих и информационно– технические инфраструктуры государства и общества (информационно-технические системы, средства работы с информацией, подразделения, коллективы и социальные системы).

Информационное оружие, воздействующее непосредственно на человека, специалисты делят на два вида.

Информационно-психологическое оружие обращено прежде всего на сознание человека и уже через него воздействует на поведение, убеждения, мотивы и потребности, нравственные установки, отношение к тому, что происходит в обществе. В качестве такого оружия могут использоваться все средства массовой информации, Интернет, публичные выступления, беседы, внушение, гипноз и т. п.

Энергоинформационное оружие воздействует на физиологию и психофизиологию человека, минуя его сознание. Человек не осознает факта воздействия, но в зависимости от его вида начинает ощущать либо бодрость, уверенность в себе, либо подавленность, тревогу, страх, агрессивность на фоне утраты способности контролировать свои действия. В природе подобное психофизическое воздействие могут оказывать, например, солнечные вспышки, влияющие на биоэлектрическую активность мозга и общее состояние человека.

В качестве источников энергоинформационного воздействия могут применяться радиолокационные системы, космические аппараты, низкочастотные и высокочастотные генераторы, биолокационные установки, химические и биологические средства и другие устройства.

Цели информационных войн и применения информационного оружия завоевание превосходства над противником и нанесение ему поражения как в конкретном акте противостояния или отдельной боевой операции, так и во внешней и

внутренней политике, экономике, обороноспособности страны в целом.

Задачи применения информационного оружия:

- подрыв международного авторитета государства, его сотрудничества с другими странами;
- манипулирование общественным сознанием внутри страны, создание атмосферы бездуховности и безнравственности, негативного отношения к национальному наследию;
- провоцирование политической напряженности и хаоса внутри страны, инициирование этнических и религиозных столкновений, забастовок, массовых беспорядков и других акций протеста;
- дезинформация населения об истории страны, о работе государственных органов, подрыв их авторитета, дискредитация всей системы управления;
- нарушение системы управления войсками, вооружением и военной техникой, объектами повышенной опасности;
- нанесение серьезного ущерба жизненно важным интересам государства в политической, экономической, социальной и других сферах деятельности.

В общей системе информационных средств особое значение имеет социальная информация – как наиболее сильное оружие и массовое средство воздействия. Именно эта информация определяет функционирование общественных образований, профессиональных, возрастных и этнических групп людей, государственных и общественных институтов, а также конкретных людей, их помыслы и поступки.

Под социальной информацией понимаются сведения, неразрывно связанные с процессом усвоения человеком знаний, жизненных норм и ценностей, побуждающих его определенным образом функционировать в обществе. К числу сущностных признаков социальной информации можно отнести следующие ее особенности:

- социальная информация всегда обращена к личности, социальным группам, классам, социуму в целом. Она является средством прямого воздействия на развитие человеческой психики, сознание человека и общества;
- социальная информация (через воздействие на общественное и индивидуальное сознание) в наибольшей степени определяет социально-экономические и политические ориентации людей во внутренней жизни государства и в отношениях с другими странами;

- социальная информация определяет эффективность передачи;
- социального опыта от поколения к поколению, сохранение и упрочение национальных традиций и обычаев;
- социальная информация в значительной мере определяет практическое поведение людей.

Эти ресурсы социальной информации можно использовать как в прогрессивных целях, так и для корыстного давления одного государства (партии, социальной группы, личности и т. д.) на другое.

Главным объектом применения социальной информации как оружия является сфера общественного сознания индивидуума и различных общностей людей, национальный менталитет, духовно-нравственные и социально-психологические качества личности и общества в целом. Определенным образом структурированная и подготовленная информация такого рода может быть исключительно сильным средством деформации индивидуального сознания, вплоть до изменения психики, доведения ее до болезненного состояния. Более того, она способна стать побудительным мотивом к суицидальным действиям, может вызвать широкомасштабные протестные действия, экстремистские выступления, террористические акты, крупные вооруженные столкновения и т. д.

При ведении информационной войны в общественное сознание народа страны, ставшей жертвой агрессии, целенаправленно внедряются такие ложные представления об окружающем мире, которые позволяют агрессору в дальнейшем свободно манипулировать как правительством, так и населением этой страны и осуществлять захват необходимых ресурсов, практически не встречая сопротивления, без применения оружия обычного типа.

Агрессивное (по целям) использование социальной информации может прикрываться лозунгами о «социально-экономической помощи», «культурном сотрудничестве» и осуществляться через управляющую «элиту» страны – жертвы агрессии, которая в меру сформированных у нее установок способна нередко искренне верить, что работает во благо своего народа.

Преимущества информационных средств противоборства в сравнении с обычным оружием:

- относительно невысокие затраты;
- лучшая возможность скрытого применения;
- размытость традиционных границ воздействия;

- отсутствие выраженного отличия мероприятий информационной войны от других видов деятельности;
- меньший риск собственного поражения; отсутствие экологического ущерба;
- возможность сохранения материально-экономической инфраструктуры.

Нередко информационное оружие называют «умным», «не смертоносным», более «гуманным». Это очень серьезное и крайне опасное по своим последствиям заблуждение. Данное оружие губительнее для людей, чем обычное средство поражения. Оно направлено против самого трудновосполнимого в человеке – его психики. И поэтому калечит людей глубже пулевого или осколочного ранения, искажая и опустошая их внутренний мир. Длительное воздействие целенаправленной дезинформацией, спланированной ложью неизбежно подавляет способность к подлинной жизни и порождает преступное поведение, наркоманию, психические расстройства, суициды.

Информационное оружие – это новый, страшный и пока еще не запрещенный вид оружия массового поражения. При нарастающей интенсивности и изощренности его применения у человечества нет будущего. Информационное оружие и смертоносно, и негуманно: оно разрушает душевную сущность человека, лишая его главной основы жизнеспособности.

Масштабность и мощность воздействия информационных факторов на психику людей выдвигают обеспечение информационно-психологической безопасности в современных условиях на уровень общенациональной проблемы. Поэтому способность защитить себя от информационной агрессии, обеспечить информационную безопасность населения становится важнейшей задачей любого государства.

1.2. Составляющие информационной безопасности

Информационная безопасность – многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только системный, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Иногда в число основных составляющих ИБ включают защиту от несанкционированного копирования информации, но, на наш взгляд, это слишком специфический аспект с сомнительными шансами на успех, поэтому мы не станем его выделять.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Наконец, конфиденциальность – это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит "руководством к действию". Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст

закона или страница Web-сервера какой-либо правительственной организации. Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность – какой смысл в информационной услуге, если она содержит искаженные сведения?

Наконец, конфиденциальные моменты есть также у многих организаций (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).

1.3. Особенности защищаемой информации

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

В соответствии со статьей 128. Гражданского кодекса РФ к объектам гражданских прав относятся вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права; работы и услуги; информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность), нематериальные блага.

Обладатель информации вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

- использовать информацию, в том числе распространять ее, по своему усмотрению;

- передавать информацию другим лицам по договору или на ином установленном законом основании;

- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

- осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации обязан:

- соблюдать права и законные интересы иных лиц;

- принимать меры по защите информации;

- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Информация в зависимости от категории доступа к ней подразделяется на:

- общедоступную информацию;

- информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- информацию, свободно распространяемую;

- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

- информацию, распространение которой в РФ ограничивается или запрещается.

Глава 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Классификация угроз информационной безопасности

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Необходимость классификации угроз ИБ АС обусловлена тем, что архитектура современных средств автоматизированной обработки информации, организационное, структурное и функциональное построение информационно-вычислительных систем и сетей, технологии и условия автоматизированной обработки информации такие, что накапливаемая, хранимая и обрабатываемая информация подвержена случайным влияниям чрезвычайно большого числа факторов, в силу чего становится невозможным формализовать задачу описания полного множества угроз. Как следствие, для защищаемой системы определяют не полный перечень угроз, а перечень классов угроз. Классификация всех возможных угроз информационной безопасности АС может быть проведена по ряду базовых признаков.

1. По природе возникновения.

1.1. Естественные угрозы-угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.

1.2. Искусственные угрозы- угрозы информационной безопасности АС, вызванные деятельностью человека.

2. По степени преднамеренности проявления.

2.1. Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала.

Например:

- проявление ошибок программно-аппаратных средств АС;
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т. п.);
- неправомерное включение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

2.2. Угрозы преднамеренного действия (например, угрозы действий злоумышленника для хищения информации).

3. По непосредственному источнику угроз.

3.1. Угрозы, непосредственным источником которых является природная среда(стихийные бедствия, магнитные бури, радиоактивное излучение и т.п.).

3.2. Угрозы, источником которых является человек:

- внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

- вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
- угроза несанкционированного копирования секретных данных пользователем АС;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

3.3. Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства:

- запуск технологических программ, способных при некомпетентном пользовании вызывать потерю работоспособности системы (зависания) или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т. п.);
- возникновение отказа в работе операционной системы.

3.4. Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства:

- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- заражение компьютера вирусами с деструктивными функциями.

4. По положению источника угроз.

4.1. Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС:

- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т. п.);
- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

- дистанционная фото- и видеосъемка.

4.2. Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС:

- хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.д.);
- применение подслушивающих устройств.

4.3. Угрозы, источник которых имеет доступ к периферийным устройства АС(терминалам).

4.4. Угрозы, источник которых расположен в АС:

- проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации;
- некорректное использование ресурсов АС.

5. По степени зависимости от активности АС.

5.1. Угрозы, которые могут проявляться независимо от активности АС:

- вскрытие шифров криптозащиты информации;
- хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем).

5.2. Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных(например, угрозы выполнения и распространения программных вирусов).

6. По степени воздействия на АС.

6.1. Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС (угроза копирования секретных данных).

6.2. Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС:

- внедрение аппаратных спецвложений, программных "закладок" и "вирусов" ("троянских коней" и "жучков"), т.е. таких участков программ, которые не нужны для выполнения заявленных функций, но позволяют преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
- действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
- угроза умышленной модификации информации.

7. По этапам доступа пользователей или программ к ресурсам АС.

7.1. Угрозы, которые могут проявляться на этапе доступа к ресурсам АС(например, угрозы несанкционированного доступа в АС).

7.2. Угрозы, которые могут проявляться после разрешения доступа к ресурсам АС(например, угрозы несанкционированного или некорректного использования ресурсов АС).

8. По способу доступа к ресурсам АС.

8.1. Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС:

- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, подбором, имитацией интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя ("маскарад");
- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.

8.2. Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС:

- вход в систему в обход средств защиты (загрузка посторонней опера ционной системы со сменных магнитных носителей и т.п.);

- угроза несанкционированного доступа к ресурсам АС путем использования недокументированных возможностей ОС.

9. По текущему месту расположения информации, хранимой и обрабатываемой в АС.

9.1. Угрозы доступа к информации на внешних запоминающих устройства (например, угроза несанкционированного копирования секретной информации с жесткого диска).

9.2. Угрозы доступа к информации в оперативной памяти:

- чтение остаточной информации из оперативной памяти;
- чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных АС и систем программирования;
- угроза доступа к системной области оперативной памяти со сторон прикладных программ.

9.3. Угрозы доступа к информации, циркулирующей в линиях связи:

- незаконное подключение к линиям связи с целью работы во время пауз в действиях законного пользователя от его имени с вводом ложных сообщений или модификацией передаваемых сообщений;
- незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений;
- перехват всего потока данных с целью дальнейшего анализа не в реальном масштабе времени.

9.4. Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере (например, угроза записи отображаемой информации на скрытую видеокамеру). Вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации АС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются следующие свойства информации систем ее обработки.

В качестве основного критерия будем использовать первый (по аспекту ИБ), привлекая при необходимости остальные. Угроза доступности (отказа служб) возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным - запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

Доступность информации– свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда возникает в этом необходимость.

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих ИС.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники. По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе. Самый радикальный способ борьбы с непреднамеренными ошибками – максимальная автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой;

- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

- отступление от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые "обиженные" сотрудники – нынешние и бывшие (они стремятся нанести вред организации-"обидчику", например: испортить оборудование; встроить логическую бомбу, которая со временем разрушит программы и/или данные; удалить данные). Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия,– пожары, наводнения, землетрясения, ураганы, по статистике, (среди которых самый опасный – перебой электропитания) приходится

13% потерь, нанесенных ИС.

Некоторые примеры угроз доступности.

Угрозы доступности могут выглядеть грубо – как повреждение или даже разрушение оборудования (в том числе носителей данных) и может вызываться естественными причинами (чаще всего – грозами). Опасны протечки водопровода и отопительной системы, в сильную жару, ломаются кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители обычно хранят небрежно, не обеспечивая их защиту от вредного воздействия окружающей среды. Перейдем теперь к программным атакам на доступность. В качестве средства вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (обычно – полосы пропускания сетей, вычислительных возможностей процессоров или ОЗУ). По расположению источника угрозы такое потребление подразделяется на локальное и удаленное. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов – атака, получившая наименование "SYN-наводнение". Она представляет собой попытку переполнить таблицу "полуоткрытых" TCP-соединений сервера (установление соединений начинается, но не заканчивается), что приводит к затруднению установление новых соединений пользователей, то есть сервер блокируется.

По отношению к атаке "Papa Smurf" уязвимы сети, воспринимающие ping-пакеты с широковещательными адресами. Ответы на такие пакеты "съедают" полосу пропускания.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме – как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание.

Для выведения систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре Pentium I дает возможность локальному пользователю путем

выполнения определенной команды "подвесить" компьютер, так что помогает только аппаратный RESET.

Программа "Teardrop" удаленно "подвешивает" компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов.

Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую, в том числе и несанкционированное изменение информации при случайных ошибках программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, периодическая запланированная коррекция некоторой базы данных).

Целостность информации - существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Обычно субъектов интересует обеспечение более широкого свойства – достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, т.е. ее неискаженности.

На втором месте по размерам ущерба стоят кражи иподлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов. В наши дни ущерб от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, знакомые с режимом работы и мерами защиты, что подтверждает опасность внутренних угроз, хотя им уделяют меньшее внимание, чем внешним.

Существует различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник может: ввести неверные данные; изменить данные.

Иногда изменяются содержательные данные, иногда – служебная информация. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) предъявила судебный иск, обвиняя президента корпорации в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное

письмо, якобы отправленное ее начальником президенту. Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что в указанное время он разговаривал по мобильному телефону, находясь вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние "файл против файла". Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарша знала пароль вице-президента, поскольку ей было поручено его менять), и иск был отвергнут...

Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить "неотказуемость", компьютерные данные не могут рассматриваться в качестве доказательства.

Потенциально уязвимы с точки зрения нарушения целостностине толькоданные, но ипрограммы. Внедрение рассмотренного выше вредоносного ПО – пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин "утечка".

Конфиденциальность информации– субъективно определяемая (приписываемая) характеристика (свойство) информации, указывающая н необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий доступа к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты их законных интересов от других субъектов информационных отношений.

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет

техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной смене только усугубляют положение, заставляя применять несложные схемы чередования или стараться свести дело к двум-трем легко запоминаемым паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая защита. Угроза же состоит в том, что кто-то не откажется узнать секреты, которые сами просятся в руки. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна – получить доступ к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Еще один пример изменения, о котором часто забывают, – хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.

Перехват данных – очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют.

Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие как маскарад– выполнение действий под видом лица, обладающего полномочиями для доступа к данным

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример – нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Таковы основные угрозы, которые наносят наибольший ущерб субъектам информационных отношений.

На современном этапе развития информационных технологий под системы или функции защиты являются неотъемлемой частью комплекса по обработке информации. Информация не представляется "в чистом виде", на пути к ней имеется хотя бы какая-нибудь система защиты, и поэтому чтобы угрожать, атакующая сторона должна преодолеть эту систему. Однако не существует абсолютно стойкой системы защиты, вопрос лишь во времени и средствах, требующихся на ее преодоление. Исходя из данных условий, примем следующую модель: защита информационной системы считается преодоленной, если в ходе ее исследования определены все уязвимости системы. Поскольку преодоление защиты также представляет собой угрозу, для защищенных систем будем рассматривать ее четвертый вид - угрозу раскрытия параметров АС, включающей в себя систему защиты. С точки зрения практики любое проводимое мероприятие предваряется этапом разведки, в ходе которого определяются основные параметры системы, её характеристики, в результате чего уточняется поставленная задача и выбираются оптимальные технические средства.

Угрозу раскрытия можно рассматривать как опосредованную. Последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность реализоваться первичным или непосредственным угрозам, перечисленным выше.

2.2. Источники угроз информационной безопасности

Все *источники угроз* информационной безопасности Доктрина подразделяет на *внешние и внутренние.*

К *внешним* источникам угроз Доктрина относит:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур против интересов РФ;
- стремление ряда стран к доминированию на мировом информационном пространстве, вытеснению России с информационных рынков;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран, нарушение функционирования информационных и телекоммуникационных систем, получение несанкционированного доступа к ним.
- К *внутренним* источникам угроз, согласно Доктрине, относятся: критическое состояние ряда отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности органов власти всех уровней по реализации единой государственной политики в области информационной безопасности;
- недостатки нормативно-правовой базы, регулирующей отношения в информационной сфере и правоприменительной практики;

- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка в России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности;
- недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов власти в информировании общества о своей деятельности, в разъяснении принимаемых решений, формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации органов власти и местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

2.3. Вредоносные программы

Вредоносные программы — одна из главных угроз информационной безопасности, что связано с масштабностью распространения этого явления и, как следствие, огромным ущербом, наносимым информационным системам.

Вредоносные программы создаются специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К указанной категории относятся вирусы и черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников.

Современное вредоносное ПО — это практически незаметный для обычного пользователя «враг», который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей. Необходимость борьбы с вредоносными программами обусловлена возможностью нарушения ими всех составляющих информационной безопасности.

Е. Касперский в своей книге «Компьютерное зловредство»[1] отмечает, что «Компьютерные вирусы, черви, троянские программы, спам, сетевые атаки и прочие нежелательные компьютерные явления давно перестали быть чем-то необычным, приводящим пользователя или системного администратора в шоковое состояние. Заражение вирусом или троянской программой — вполне частая

ситуация как для тех, кто небрежно относится к элементарным правилам компьютерной гигиены, так и для профессиональных системных администраторов, отвечающих за бесперебойную работу корпоративных сетей. Обыденным также стал электронный спам, давно количественно перекрывший поток «легальных» писем».

ЗАКЛЮЧЕНИЕ

Угроза защищаемой информации – совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации.

Самым опасным источником дестабилизирующего воздействия на информацию является человек, потому как на защищаемую информацию могут оказывать воздействие различные категории людей.

Разнообразие видов и способов дестабилизирующего воздействия на защищаемую информацию говорит о необходимости комплексной системы защиты информации.

Современная Доктрина информационной безопасности Российской Федерации наиболее полно раскрывает виды и источники угроз информационной безопасности, а также методы обеспечения информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Барабанов А. С. Инструментальные средства проведения испытаний систем по требованиям безопасности информации. М.: Защита информации. INSIDE, 2011. — с. 24−36.

2. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010. — с. 124−129.

3. Гладких А.А., В.Е. Дементьев / Базовые принципы информационной безопасности вычислительных сетей: учебное пособие для студентов;

Ульяновск: изд-во УлГТУ, 2011. — с. 18−31.

4. Ерохин В. В., Погонышева Д. А., Степченко И. Г. Безопасность информационных систем. Учебное пособие. — М.: Флинта, Наука, 2015. — с. 85−89.

5. Мельников Д. А. Организация и обеспечение безопасности информационно-технологических сетей и систем. — М.: КДУ, 2015. — с. 147−149.

6. Оголюк А.А., А.В. Щеглов / Технология и программный комплекс защиты рабочих станций. — М.: изд-во Финансы и статистика, 2011. — с. 252−265.

7. Петренко С.А., Симонов С.В. /Управление информационными рисками. Экономически оправданная безопасность — М.: Радио и связь, 2012. — с. 187−193.

8. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 2014. — с. 63−71.

9. Симонов С.В. Технологии аудита информационной безопасности // Конфидент. Защита информации. — № 2. М.: Издательство СИП РИА — 2013. — с. 12−30.

10. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий / Под общ. ред. В.А. Галатенко. — М.: Издательство СИП РИА, 2011. — с. 85−101.

11. Храмов В.В. Информационная безопасность и защита информации Методическое пособие. — Ростов на Дону.: РГУПС, 2011. — с. 74−100.

12. Шахалов И.Ю. Лицензирование деятельности по технической защите конфиденциальной информации. — М.: Вопросы кибербезопасности, 2013. — с. 121−130.

13. Щеглов А.Ю. / Защита информации он несанкционированного доступа. — М.: изд-во Гелиос АРВ, 2014. — с. 203−210.

14. Официальный сайт первого в России независимого информационно-

аналитический центра [Электронный ресурс].